A SYSTEM AND METHOD FOR ENROLLING IN A BIOMETRIC SYSTEM

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation-in-part of application no. 10/251,305, filed September 20, 2002, which claims domestic priority from provisional application no. 60/324,229, filed September 21, 2001. The 10/251,305 and the 60/324,229 applications are each incorporated by reference herein, in its entirety, for all purposes.

FIELD OF THE INVENTION

[0002] This application relates generally to the method of enrolling information into a system for biometric recognition/verification. More particularly, the present invention relates to an atemporal method for enrolling portions of enrollment information in a system for biometric recognition and/or verification.

BACKGROUND OF THE INVENTION

[0003] Generally, systems that provide biometric recognition and/or verification for verifying an individual's identity, verifying an individual's age, or authorizing a financial transaction require that a system user undergo an enrollment. In an enrollment, the individual typically presents identity verifying information, documents to attest to his true identity, and one or more biometric scans. Biometric information is then presented in subsequent transactions to recognize or verify the user and to indicate to the system that the individual has undergone enrollment. This biometric information may additionally be used to alert the system to various individual privileges, preferences, limitations, and/or warnings that are indicated in the user's record and relate to that system user.

[0004] There are two main types of biometric comparison systems: biometric verification systems, where the system performs a "one-to-one" comparison of an individual's biometric to a record of her biometric, and biometric recognition systems, where the system performs a "one-to-more than one" biometric comparison of an individual's biometric to multiple

biometric records. A "one-to-one" biometric comparison verifies the individual presenting the biometric is who he says he is, and a "one-to-more than one" biometric comparison recognizes an individual's biometric from a group of two or more biometrics. For the purposes of this application, "biometric system" is intended to refer to both one-to-more than one biometric systems and one-to-one biometric systems.

[0005] The problem with current methods of enrolling system users in biometric systems is that those methods force enrollees to enter all of their enrollment information at once. Because of the range of differing biometric systems and the differing enrollment requirements of each, it's problematic to expect enrollees to enter the entire enrollment data needed to allow them to use the system at once because they may not know the enrollment data they need to present at the time of enrollment. What is needed are better systems and methods for enrolling users to help streamline and improve the enrollment process.

SUMMARY OF THE INVENTION

[0006] The present invention addresses the aforementioned needs by providing a convenient method of enrolling individuals to use biometric identification/verification systems. A flexible process by which individuals can enter the enrollment information needed to activate the user enables individuals and/or groups to interact with the system at their availability and convenience.

BRIEF SUMMARY OF THE DRAWINGS

[0007] **FIG. 1** illustrates an overview of the general architecture of a system for enrolling a potential system user to use a biometric system according to an embodiment of the present invention.

[0008] **FIG. 2** illustrates a flowchart of a process for pre-enrolling information into a system for verifying identity through biometric recognition/verification.

[0009] **FIG. 3** illustrates a flowchart of a process for enrolling information that enables a system user to verify his identity through biometric recognition/verification in a biometric

system.

[0010] **FIG. 4** illustrates a flowchart of a process for enrolling information that enables a system user to verify his identity through biometric recognition/verification in a biometric system.

DETAILED DESCRIPTION OF THE INVENTION

[0011] Additional objects and advantages of the present invention will be apparent in the following detailed description read in conjunction with the accompanying drawing figures.

[0012] As previously noted, the present invention encompasses a system and method for enrolling a potential user in a system for verifying identity through biometric recognition/verification. The disclosed enrollment method allows individuals to enter enrollment information into a system over multiple system accesses. Such an enrollment method provides individuals with an accessible and forgiving method of presenting information into a biometric system. Whereas conventional methods of enrollment into a biometric system demand the total enrollment information all at once, the disclosed method allows individuals to enter enrollment information into a biometric system at their availability and convenience.

[0013] **FIG. 1** illustrates a general architecture overview of an identity verification system **100** that is based on biometric recognition/verification. As will be described in greater detail below, identity verification system **100** enables a flexible enrollment process by which users are encouraged to provide registration information. This registration information is stored in at least one system database **102**, **124** where system user records are stored. In one embodiment, the system database is a central database to which all system user records are stored and from which informational system user records are accessed for identity verification. In another embodiment, the system database is one or more operator databases **124** to which a select set of system operator records are stored and from which a select set of system operator records are accessed for identity verification. In an additional embodiment, identity verification system **100** may also utilize a combination of central databases **102** and

one or more operator databases **124**. In general, embodiments utilizing a combination of system databases **102**, **124** enable increased control of information flow throughout identity verification system **100**. As described in greater detail below, various examples of information flow configurations within the system can include "open," "closed," and "multiple system operator" system models. In still further embodiments, system database **102**, **124** can further comprise one or more sub databases that are contained within a particular system database **102**, **124**. In such embodiments, system user data, system operator data, and other system data may be distributed across multiple databases within the system database.

[0014] A system user record holds system user recognition/verification and identity verifying information related to an individual seeking biometric recognition/verification so that the system user may identify himself with the system. The information held in such a record may include, by way of illustration and without limitation, a system user's government identification number(s) and corresponding state(s) of issue, home address, and a telephone number and at least one biometric record. A system user may present any number of identity verifying documents or testaments to his identity depending on the embodiment of the biometric system. By way of illustration and not of limitation, examples of such documents or testaments include a financial token, a digital image, a video clip, family information, or a DNA sample. Depending on the particular implementation, a system user record can also hold financial account information and/or a system identification number (SID). A SID is a code used in conjunction with a system user biometric scan for biometric recognition/verification. In an alternate embodiment, a system user may create a SID during a pre-enrollment session and then use that SID to identify himself during subsequent system accesses.

[0015] Additionally, system user records are marked according to various pre-active states of activity before the records have been enabled for use and have been marked active for use in a biometric identification/verification system. Such pre-active states may include but are not limited to idle pre-active, current pre-active, and bad pre-active. Idle pre-active system user records include those where a system user partial record has been created and the record

has not been augmented or enabled. Current pre-active system user pre-enrollment records include those where a system user partial record has been created and the record is augmented on a regular basis. Bad pre-active system user records include those where a system user partial record has been created but fraud regarding information presented for storage or stored in that record has been detected. After a system user record includes enabling enrollment information, the system user record is marked active, and a history of the record's pre-active activity states is stored in the system user record. In an additional embodiment, system user records that are enabled and are marked active are also marked as verified or self-enrolled. Verified records are those that have been reviewed and verified by at least one system operator, third party, and/or third party database. Self-enrolled records are those that contain the necessary enrollment data needed to enable their respective system users to identify their identities in the system but that have not been verified.

[0016] System operator records hold information useful for authenticating an operator, such as a name or ID number, an address, and a phone number. In an alternate embodiment of the present invention, the operator records also hold employer information if the operator is an employee of an employer who is also an operator. In another embodiment of the present invention, operator records hold an operator SID and/or an operator biometric scan.

[0017] The system may be configured so that at least one system database **102**, **124** is connected to at least one network **101**, such as but not limited to, the Internet. This network comprises connections to at least one device where a system user may enter pre-enrollment information. These devices include but are not limited to a vending machine **110**, a kiosk **120**, a personal computer **104**, an enrollment desk **126** or a wireless device **114**, connected via wireless network, with or without respective biometric input devices (BIDs) **112**, **122**, **106**, **128** and **116**. The network also comprises connections to one or more enrollment desks **126** with connected BIDs **128** where system users may enable their enrollment records by presenting the remainder of system user information needed to allow the system user to use the system and where the enabling system access is monitored and verified by a system operator. The network also comprises connections to devices where system users may enable their enrollment records via synchronous or asynchronous operator observation and

verification, such as a kiosk **120** with attached BID **122** and/or a vending machine **110** with attached BID **112**.

[0018] Networks used in additional embodiments include LANs (local area networks), WANs (wide area networks), telephone networks and parcel delivery systems, such as but not limited to, the United States Postal Service, United Parcel Service, and Federal Express. In such embodiments, system users communicate with at least one system database **102**, **124** via telephone **136** or fax **132**, both which may or may not have connected BID devices **138** and **134**, respectively. Such embodiments also allow system users to communicate with a system database via mail or parcel service **130**.

[0019] Additional embodiments of the system also comprise connections to one or more third party sources, such as a third party database **118** and/or one or more financial institutions **140,** in which system user-presented information is verified and/or from which system user information is pulled. Pre-enrollment and enrollment enabling devices compose pre-enrollment and enrollment enabling stations, respectively. Stations are composed of at least one pre-enrollment device and the necessary means for sending and receiving information to and from a system user and to and from a system database.

[0020] In one embodiment, the system is configured as an "open" system, meaning all information entered into the system is transmitted to and stored in a centralized system database **102**. An open system allows system users to conduct enrollments at any enrollment station in the system because an open system shares system user information stored in the centralized system database **102** with all enrollment stations.

[0021] In an alternate embodiment, the system is configured as a "closed" system, meaning information entered into the system via a specific operator device is transmitted to and stored in a system database specific to that operator **124**, and this information is not shared with other enrollment stations or other system databases. This is referred to as a "closed" system because system users who enrolled in one system operator's database **124** must enroll in the database of each additional system operator system wherein they would like to enroll their information. Operator system databases **124** in closed systems may query other databases, such as a third party information database **118**, for system user information

verifications. However, all system user information that is enrolled into a particular operator system database **124** is stored in that database. In an alternate embodiment of the closed system, information pertaining to specific system operators is stored in a partitioned, central system database **102**. System operator related information is stored in system, operator-specific partitions and is closed to all other system operators. Only the system operator and system operator employees may access that partition of the central system database **102**. In yet an additional embodiment, system operator related information stored in an operator system database is additionally stored on the central system database **102** where their system users' records are stored. Such an embodiment is useful for information protection in the event database information is lost.

[0022] In a further embodiment of the present invention, system user information is stored in select system multiple-operator databases or select, system multiple-operator partitions within the central system database **102**. In this embodiment, a group of system operators share data with each other and they choose whether or not to share system information with other system operators within the system. Such a system is referred to as a "multi-operator" system. This system allows a chain of system operators owned by the same entity or linked in some other manner to share system user enrollment information amongst them without sharing that information with all other non-designated system operators registered in the system. Information in such a system may be shared between operator system databases **124** and the central system database **102** freely or sharing may be monitored by rules set in the operator system databases **124**, the central system database **102**, or both. By way of illustration and not as a limitation, one system operator might only want to share system user enrollment information with one of five system operators in a multi-verifier system or all system operators might not want to send or store system user enrollment information to the central system database **102**.

[0023] The configuration of the system as an "open" system, "closed" system, or "multi-operator" system illustrates various ways of implementing the principles of the present invention. System configuration might be determined by the system in which the enrollment information is used. For example, a merchant who is an operator in the system and who

conducts biometrically authorized customer loyalty programs might have a system configured with his own operator system database **124** and one or two biometric authorization terminals connected to that database. In this system configuration, the merchant's database files only exist on his database **124** and are retrieved or accessed for biometric matching only by the one or two pre-determined stations connected to the database **124**; therefore, the system would be a "closed" system.

[0024] Referring to **FIG. 2**, a flowchart of a process for pre-enrollment into a system for verifying identity through biometric recognition/verification is illustrated. For the purposes of this application, "pre-enrollment" is defined as providing less than the complete information required to enable usage of a system for biometric recognition/verification. As would be appreciated, determining the data required to enable usage of the system would depend on the embodiment of the system in which the individual is enrolling. For accessibility purposes, it is conceived that individuals may pre-enroll information into the system at their convenience.

[0025] At step **202**, a system user is prompted to present a chosen portion of the data necessary for enabling usage of the biometric system. System users may pre-enroll as much or as little of the information as they wish, or as predetermined by the system. In an additional embodiment, the system may require or prohibit a system user from entering specified information during pre-enrollment. For example, a system user may be required to pre-enroll via a device **110,120,126** connected to a BID **112,122,128**, where the system user must present a biometric scan. The system may also set other pre-enrollment restrictions, such as requiring a system user to sufficiently provide enabling enrollment information, any information not provided during a pre-enrollment access but needed to mark a user's system user record as active, within a set timeframe. Additionally, the system may be configured to allow a system user to enter pre-enrollment information in multiple system accesses or may require the system user to enter all specified pre-enrollment information during one system access.

[0026] At step **204**, pre-enrollment information that the system user presents is sent to the system database for storage. In one embodiment, if the presenter sends her pre-enrollment

information via print form through couriers, such as the United States Postal Service, the presenter's information is scanned or hand-keyed into the system database for storage. At step 206, the pre-enrollment information is stored for later pre-enrollment access and/or enabling-enrollment retrieval.

[0027] Pre-enrollment records are stored as partial records that cannot be used to identify a system user until the identified remainder of the system user enrollment information is stored in the system. Such partial records are marked in some manner to denote that the records are incomplete. Pre-enrollment records are stored in the system database but may be accessed by the system user for pre-enrollment information augmentation or by a participating system operator for enabling enrollment. System users may augment their pre-enrollment records during subsequent pre-enrollment accesses by presenting any portion of previously enrolled information into the system for identification and then presenting the desired augmenting information. It should be noted that a system user may augment his pre-enrolled information as often as he wishes during the pre-enrollment stage.

[0028] According to a closed embodiment of the system, pre-enrollment records are stored in one or more specified operator system databases **124**. Such an embodiment asks system users to choose an operator system database with which to store their pre-enrollment information. According to a multi-operator embodiment of the system, system users select one or more chains of system operators with which to share their pre-enrollment record. Both closed and multi-operator systems may be configured to additionally store system user information in the central system database **102** and/or one or more operator system databases **124**.

[0029] In an alternate embodiment of pre-enrollment, potential system user information is retrieved from a third party database **118**. This information retrieval may be prompted by the system user or may be automated by the system. The third party database **118** may be for example an employer database, where information on all of that employer's employees is stored. A system user prompts retrieval of his information from a third party database **118**, where his information is held, during either a pre-enrollment system access or an enabling access. He does so by providing information about the third party database **118** and an

indicator. A system user identifies the third party database **118** that he wants the system to access for retrieving information by a means such as providing the enrollment station with the name of the entity with which the database is held. The indicator may include by way of illustration and without limitation a password that the system user has specified with the third party database **118** to indicate that he authorizes the system database pulling his information.

[0030] Information is automatically retrieved in a manner such as pulling the information from a purchased or acquired database. By way of illustration and not as a limitation, the system database operator could purchase driver's license data from a state or government database and save that information as pre-enrollment records. In an alternate embodiment, information obtained from third party databases **118** may also be used to verify information potential system users enter during pre-enrollment or enrollment enabling. This information could be easily entered into a system database **102,124** so that when system users, whose information was recorded in a system database **102,124** want to pre-enroll or enable enrollment in the system of the invention, some or all of that information contained within the third party database **118** would already be recorded within the system.

[0031] In an additional embodiment, the pre-enrollment information presented by the system user may be evaluated by a system database **102,124**, one or more system database managers, or one or more system operators in an effort to run preliminary identity verifications on a system user before they attempt to enable enrollment. These preliminary identity verifications include but are not limited to using pre-enrollment information to check a system user's credit history; to verify identity documents presented during pre-enrollment; to verify presented information with third party databases **118**; to verify financial account information by pre-noting the financial account through the Automated Clearing House (ACH) system; to verify financial account information by depositing an amount of money into a financial account, that amount serving as the system user's identification number within the system; to confirm presented information via an email or the US Postal Service; or to contact one or more third parties whose information was provided by the system user for system user identity verification. Results from these

preliminary identity verifications are stored in the system user's record and used to evaluate the system user's enrollment enabling access. In an additional embodiment, system users can also re-present information that did not pass preliminary verification. The system user may re-present this information during another pre-enrollment access or an enrollment enabling access. Additionally, if the system user has enabled her system record and some portion of her information is not verified, the system may contact the system user and request her to re-present this information via a specified manner.

[0032] An additional feature of the present invention includes the system rendering incentives to system users for providing pre-enrollment information. In such an embodiment, the system may offer system users incentives for pre-enrolling to entice them into presenting a portion of enrollment information. For example, a vending machine stocked with incentives may be equipped as a pre-enrollment station. When a system user pre-enrolls her name in the system, the machine dispenses an incentive. Additionally, the system may offer incentives for augmenting information system users present after their initial pre-enrollment access in a subsequent pre-enrollment access. The machine might also notify the system user that if she augments her name data with her address and telephone number, she will receive another incentive. This would enable the system to further entice the now pre-enrolled individual to present even more information toward enabling her system user record and receive additional incentives in exchange for presenting that information.

[0033] Methods of rendering incentives within the system vary, but often the configuration of the pre-enrollment station determines the method in which incentives are rendered. For example, pre-enrollment devices such as vending machines are equipped to render incentives directly. This can be done by the system signaling a vending machine to directly dispense a pre-determined item. Other methods of rendering incentives include but are not limited to automated deposits, certificate print-outs and delivery through a parcel delivery service. Examples of automated deposits include direct automated deposits where a system user has registered financial account information with the system, and the system electronically credits the system user's financial account with a pre-determined monetary

amount. Incentives are also rendered via automated deposits to the system user's system record. A rendering note is stored in the system user's record and the system user may retrieve that incentive at any system-determined point of retrieval. For example, a participating merchant in the system allows a system user to access her system record and one or more incentives stored therein are redeemed with the merchant for pre-determined or system-user-selected items. Incentives are also rendered via print-outs. This method of incentive delivery is most applicable in rendering incentives that cannot be directly dispensed or electronically delivered. For example, a registration station is equipped with a printing device and it prints a gift certificate, coupon, discount, and/or redemption number and redemption instructions. Incentives are also deliverable via a parcel delivery service.

[0034] In an additional embodiment, the system allows the system user to select from two or more incentives. Systems that allow system users to choose an incentive from a number of choices serve a two-fold purpose. One, they provide a greater response from the system user by providing him with a choice of incentive, thereby increasing the chance that the system is offering him something he might want. Two, this method also allows the system to obtain further information about the user by profiling him according to his incentive selection, which helps the system determine his likes, needs and wants. Such information might also be useful in determining a personalized incentive selection that would entice the system user to present even more information into the system. Such system configurations also allow the system to conduct market research by asking a system user feedback questions in subsequent accesses about the incentive(s) he received on his last system access.

[0035] Referring to **FIG. 3**, a process for enrolling information that enables a system user to verify his identity through biometric recognition/verification in a biometric system is illustrated. At step **302**, the potential system user who wishes to enroll enabling information in the system and who has already provided a portion of the necessary enrollment information during manual or automatic pre-enrollment presents at least one portion of the pre-registered information. By way of illustration and without limitation, information that might be entered to identify the system user may be a telephone number, a name, a

biometric, a driver's license number, or a social security number that the system user pre-enrolled in the system. At step **304**, the system user is then prompted to enter any enrollment information that he did not enter during pre-enrollment. At step **306**, the information entered is sent to a system database **102,124** where, at step **308**, it is stored with its matching pre-enrollment record. If enrollment enabling parameters are met, the record is marked as enrolled and as active in the system. The system user may then use his record for biometric related transactions.

[0036] In an additional embodiment, the system evaluates enabled system records to ensure that they contain the necessary information for fully enrolling a system user to use a biometric system. If, during this evaluation, any information is missing from or is unverified in a system user record, the system user is offered an opportunity to enter the missing information indicated by the system or correct previously entered information that is not verified. Further, the system may be configured to allow system users to review information that they entered into the system during any system access or any information pertaining to them that was provided by a third party information database. This information may be displayed to the system user via electronic display during a pre-enrollment access or enrollment enabling. If any information displayed to a system user is incorrect, the system user indicates this to the system in some manner via keypad and then corrects the incorrect information.

[0037] In an additional embodiment of enrolling enabling information, a system user's record retains an inactive status until information the system user entered is verified with one or more third party sources. This embodiment assures that both pre-enrollment and enrollment enabling information is verified. Further additional embodiments may only verify specific information that typically requests higher security, such as financial account information. Once the necessary information is verified, the system user's record is marked active. If, during verification, a portion or all of a system user's information is not verified, a system manager and/or system operator contacts the system user to notify her that she must re-present the unverifiable information. Depending on the embodiment of the invention, the system user may re-present the unverifiable information via any enrollment

device.

[0038] Referring to **FIG. 4**, a process for enrolling information that enables a system user to verify his identity through biometric recognition/verification in a biometric system. At step **402**, the potential system user who wishes to complete enrollment and who has already provided a portion of the necessary enrollment information during manual or automatic pre-enrollment presents at least a portion of the pre-registered information. By way of illustration and without limitation, information that might be entered to identify the system user may be a telephone number, a name, a biometric, a driver's license number, or a social security number that the system user pre-enrolled in the system. At step **404**, the information the system user enters is sent to a system database **102,124**. At step **406**, the pre-enrollment record linked to the information sent to the system database is evaluated to determine what information is needed to enable the system user to use the system and at step **408**, a request for that information is sent to the enrollment device **110,120,126**. At step **410**, the system user presents the requested information, and at step **412**, all entered information is sent to the system database where at step **414**, it is stored with its matching pre-enrollment record. Once the record contains enrollment enabling information, the record is marked as enrolled and is marked active within the system.

[0039] Both methods of enabling enrollment might further include offering pre-enrolled system users incentives to provide enabling information. Such an embodiment would entice pre-enrolled system users to present enabling information into the system sooner than the system user anticipated.

[0040] In an additional embodiment, system operators provide pre-enrollment verification and/or enrollment enabling verification. An operator may provide verification in numerous ways. In the simplest form of operator verification, the operator identifies herself to the system to show the system that she is present at the pre-enrollment station and/or enrollment enabling station. The operator may identify herself in a manner such as pressing a designated key on the station device, entering an operator code, or entering operator-specific identity information such as an operator biometric sample. The system can more easily track and monitor an operator's verifying behavior if the operator presents operator-specific

information. In a system embodiment with higher security requirements, operators review the information a system user presents during a pre-enrollment and/or enrollment enabling and signal verification of the information presented. This signal might mean that the verifier only glanced over system user identity documents to make sure they looked authentic. The signal could alternatively comprise more complicated methods of verification such as a system operator contacting a credit database to verify the system user's credit history based upon an identity document the system user present during the enrollment. In a further embodiment, system operators may also verify enrollment from a remote device. Such enrollment verification can be done in a real-time evaluation set-up, where system user information is verified during the same system access in which it is entered, or enrollment verification can be done atemporally, where system user enrollment information is verified at some point after he has entered his enrollment data but before his record is marked active. In either case, in such an embodiment, the system user would not be able to use his system user record until his enrollment information had been verified according to system-based parameters. In a further embodiment, an enrollment is verified by an automated operator, which would use a special code to identify itself to the system that would indicate that it is an automated verifier. Regardless of the method of operator verification of a system user's presented enrollment information, operator verification indicators are stored in the system user records in which they verify information. The system may also reward system operators who verify system user information by offering operators incentives for persuading system users to take action within the system. For example, a system operator might be offered an incentive for every fifty system users they persuade to enable enrollment in the system.

[0041] In an additional embodiment, system users may pre-enroll, enable enrollment, and their system record may be marked active upon enrollment enabling without their enrollment information being verified by a system operator. In such an embodiment, the system user's record would be marked to denote that she is conducting transactions in the system as a self-enrolled system user. A self-enrolled system user might be restricted from performing certain transactions and may be required to re-represent a portion or all of her enrollment information to conduct those transactions. Once a system operator verifies a

self-enrolled system user, the system removes the self-enrollment mark from the system user's enrollment record.

[0042] In an additional embodiment, information transferred between two points in the system is encrypted. For purposes of example and without limitation, information may be encrypted at one point and sent across a non-secure connection between the points or not encrypted at a point of communication and sent to the other point of communication across a secure connection. Encryption and decryption of these messages may be monitored by services provided by a company such as VeriSign. As an added level of security, one alternate embodiment encrypts even information internal to a terminal and which is never transmitted in a communication. This prevents retrieval of sensitive information (*e.g.*, data corresponding to a biometric scan) from a stolen terminal. In an additional embodiment, the system incorporates one or more anti-tampering methods by which to recognize authentic and non-authentic system requests.

[0043] According to another embodiment, pre-enrollment and/or enrollment completion procedures may additionally comprise providing system users with printed or electronic records of their system access. The electronic records may take various forms such as but not limited to a media output to a personal data assistant, a smartcard, a cell phone, and an email address. Information included in these reports may be any information pertinent to the system access performed, such as access date and time, a transaction number, enrollment information enrolled during pre-enrollment, necessary enrollment information to complete an enrollment, instructions on how to complete a pre-enrollment, information on where to complete an enrollment, and/or instructions on how to contact customer service.

[0044] It is also an alternate embodiment of the present invention to provide operators with system user and other operator profile reports in case of suspected fraudulent activity within the system. These reports may be customized to display selected information from a system user's or system operator's record.

[0045] According to another hybrid embodiment, the system may be configured to send an identification number associated with a pre-enrollment/enrollment device (*e.g.*, terminal

identification number or serial number) and/or connection (*e.g.*, internet protocol address) along with pre-enrollment or enrollment completion information. Such an embodiment is conceived to increase system security.

[0046] A system and method for pre-enrolling in a biometric system has been illustrated. It will be appreciated by those skilled in the art that the system and method of the present invention can be used to perform more convenient enrollments into biometric systems. It will thus be appreciated by those skilled in the art that other variations of the present invention will be possible without departing from the scope of the invention disclosed.

[0047] These and other aspects of the present invention will become apparent to those skilled in the art by a review of the following detailed description. Although a number of salient features of the present invention have been described above the invention is capable of other embodiments and of being practiced and carried out in various ways that would be apparent to one of ordinary skill in the art after reading the disclosed invention, and therefore the above description should not be considered to be exclusive of these other embodiments. Also, it is to be understood that the phraseology and terminology employed herein are for the purposes of description and should not be regarded as limiting.